California Joint Cyber Incident Response Guide

California Office of Emergency Services

California Cyber Security Integration Center

Version 1.3a 8/2/2021

Page Intentionally Left Blank

Table of Contents

Table of Tables

Overview

Cyber incidents are typically non-discriminatory and can affect any and all agencies, companies and businesses within the State of California either directly or indirectly. Cyber preparation and vigilance are key to ensure an acceptable level of security is established before, during and after an incident. Balancing cybersecurity with business operations is vital to business continuity.

When a privacy or information security incident occurs, it is imperative that the responsible entity follow documented procedures for responding to the incident. An Incident Response Plan (IRP) is intended to meet this requirement. The IRP should be in both hard copy and electronic formats and be readily available to those involved in the response, including members of the Incident Response Team (IRT) and others that may play a significant role in the response such as Public Information Officers, Management Teams and Privacy Officers.

Two principles guide the establishment of the IRP. First, every entity must establish in advance a plan for responding to an incident as well as procedures to maintain the plan. Second, each entity should test and update the plan periodically to ensure that it is appropriate, functional and up-to-date.

To facilitate incident response operations, responsibility for incident handling operations should be assigned to the IRT. In the event that an actual or perceived cyber incident occurs, the members of this team will execute the IRP. To ensure that the team is fully prepared for its responsibilities, all team members should receive training in incident response operations within 6 months of appointment to the team and thereafter on an annual basis.

Entities should test the incident response plan annually through the use of tabletop exercises, simulation tests and, at a minimum, a full test every three years. Where appropriate, organizations should integrate these tests with the testing of related plans such as the organization's Business Continuity Plan, Technology Recovery Plan, Disaster Recovery Plan, etc. The results of these tests will be documented and shared with key stakeholders.

Incident Response Plans should be reviewed and revised on an annual basis, based upon the documented results of previously conducted tests or reviews of actual incidents and execution of the IRP. Upon completion of plan revision, updated plans should be distributed to all IRT members and other stakeholders.

The California Cybersecurity Integration Center (Cal-CSIC)

The California Cyber Security Integration Center (Cal-CSIC) is the State's information clearing house for cybersecurity information and whose primary mission is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector networks.

The Cal-CSIC was established by Governor Edmund G. "Jerry" Brown, Jr. through Executive Order B-34-15 and comprised of cybersecurity experts from its original strategic core partners that include the Governor's Office of Emergency Services (Cal OES), the California Department of Technology (CDT), the California Highway Patrol (CHP) and the California Military Department (CMD). The Cal-CSIC also includes Cybersecurity specialists from the Federal Bureau of Investigations (FBI), the United States Department of Homeland Security (DHS) and liaises with many other federal, state, local and private sector cybersecurity experts. The Cal-CSIC serves as the central organizing hub for sharing of cyber threat intelligence as well as coordinating incident response activities with public and private entities across the state.

The Cal-CSIC's mandate is to share cyber threat information across not just State partners, but also amongst local, tribal, educational and private sector entities to protect the state from cyberattack, including cyberattacks on critical infrastructure. The Cal-CSIC ingests, analyzes, and prioritizes cyber threats and sends alerts to California's cybersecurity stakeholders when threats may damage California's economy, critical infrastructure, and computer networks, or wreak havoc on its citizens.

The Cal-CSIC coordinates cyber incident response for incidents that may exceed the capability and resources of local jurisdictions or for large cyber incidents such as when a cyber incident causes the state to implement its State Emergency Plan, specifically Emergency Support Function 18 (ESF-18). The Cal-CSIC, through its core partners, provides technical support for detection and remediation of cyber incidents as well as provides best practice recommendations to prevent or minimize the impact of future cyber incidents.

The California Governor's Cybersecurity Task Force

The Cal-CSIC was originally recommended to the Governor by the Governor's Cybersecurity Task Force. To address the growing cyber threat to networks, personal privacy, and critical infrastructure, Governor Brown directed his Office of Emergency Services and the California Department of Technology to establish the California Cybersecurity Task Force. The California Cybersecurity Task Force is a statewide partnership comprised of key stakeholders, subject matter experts, and cybersecurity professionals from California's public sector, private industry, academia, and law enforcement. The Task Force serves as an advisory body to the State of California Senior Administration Officials in matters related to Cybersecurity. By fostering a culture of cybersecurity through education, information sharing, workforce development and economic growth, the Task Force hopes to advance the State's cybersecurity and position California as a national leader and preferred location for cyber business, education, and research.

General Guidance

This document is designed to assist governmental and non-governmental entities within California, including State, Local, Tribal, Territorial and Private Sector (SLTTP) understand the importance of establishing and maintaining an Incident Response Plan (IRP) and incident response capabilities, including an Incident Response Team (IRT).

Understanding how to react to an incident depends on understanding the organization's mission and the mission critical systems required to meet the organization's business objectives and the threat environment. Each organization should also regularly review their critical business systems and applications. The reviews are typically conducted annually to ensure applications and systems are still relevant for business operations.

Lines of Effort

Today's cyber dependent environment necessitates that public and private sectors vigilantly manage, respond to, and investigate cyber incidents, and share lessons learned or Indicators of Compromise (IOC's) so that others can minimize the potential damage to their information systems and data. Ensuring unity of effort during incident response requires a shared understanding of roles and responsibilities for all participating organizations throughout the cyber incident lifecycle.

There are four lines of effort in cyber incident response: Threat Response, Asset Response, Intelligence Support, and Affected Entity Response. Table 1 provides a summary of the entities typically involved in each line of effort. These concurrent lines of effort provide the foundation required to synchronize various response efforts before, during and after a cyber incident.

Line of Effort	Possible Participating Entities
Threat Response	Local Law Enforcement, CHP Cyber Crimes Investigation Unit (CCIU), and FBI Cyber Division
Asset Response	CDT-SOC, Cal-CSIC, and 3rd-Party Cybersecurity resources
Intelligence Support	Cal-CSIC, CHP CCIU, FBI Cyber Division, Multi-State Information Sharing & Analysis Center (MS-ISAC). and 3rd-Party Cybersecurity resources
Affected Entity Response	Entity Information Security Officer (ISO), Information Technology (IT) staff, management teams, cybersecurity staff, and 3rd-Party Cybersecurity resources

Table 1 - Response Lines of Effort

In alignment with Presidential Policy Directive 41[1], threat response, asset response and intelligence support are adopted and defined as:

Threat response activities include the appropriate law enforcement investigative activities for;

- collecting evidence and gathering intelligence to provide attribution

[1] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

- linking related incidents and identifying additional possible affected entities
- identifying threat pursuit and disruption opportunities
- developing and executing courses of action to mitigate the immediate threat and facilitating information sharing and coordination with asset response efforts.

Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents by;

- identifying other entities possibly at risk and assessing their risk to the same or similar vulnerabilities
- assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks
- facilitating information sharing and operational coordination with threat response
- providing guidance on how best to utilize State and local resources and capabilities in a timely, effective manner to speed recovery.

Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available State and local resource capabilities; and facilitating information sharing and operational coordination with other entities.

Intelligence support facilitates the building of situational threat awareness and sharing of related intelligence to;

- create an integrated analysis of threat trends and events
- identify and assist with the mitigation of knowledge gaps
- suggest methods to degrade or mitigate adversary threat capabilities.

An affected entity is highly encouraged to share information surrounding the event with other cybersecurity specialists to assist with the investigative, analysis, response and recovery phases of cyber incident response. State of California entities have mandatory reporting requirements, see the California Joint Cyber Incident Communications Framework. The affected entity is the data owner and retains responsibility to ensure appropriate actions and safeguards are in place to remediate threats and secure their information.

Incident Response Lifecycle

A security incident response capability will be developed and implemented for all information systems that house or access information vital to the economic, financial, and / or operational stability to the people of the State of California. An incident response capability should include a defined plan and address the following stages of incident response:

1. Preparation
2. Detection
3. Analysis
4. Containment
5. Eradication
6. Recovery
7. Post-Incident Activity
8. Other Response Activities

The organization is responsible for understanding the indicators, interpreting agency and external inputs, as well as conducting all required coordination necessary to support Cyber incidents reported by State and Non-State agencies.

The organization receives, reviews, and analyzes the event indicators from multiple sources to determine the nature and severity of the event(s) in question. The information derived from the data analysis is then used to inform the partners of the potential or current threats, as well as coordinate all necessary remedial efforts required to return operational stability to the partner agencies.

1 Preparation

Incident handling requires great consideration and coordination prior to event handling in order to ensure as many circumstances as possible are addressed prior, during and after the event. These include, but are not limited to Plans and Policy, Resources, and Personnel.

1.1 Plans and Policy

Planning begins with the development of the Incident Response Plan (IRP) and training an Incident Response Team (IRT) or identifying outside resources for a 3rd-Party IRT. When outsourcing an IRT, the 3rd-Party organization should be pre-identified and contracted. Ideally the contract should be in place before a cyber incident occurs. The 3rd-Party should already perform a review of the customer organization's IT infrastructure, review and test the IRP, and clearly establish a Service Level Agreement between all parties.

The Planning phase also includes training for rank and file employees as well as supervisors and managers. They should be trained to identify suspicious behavior, whether it's the computer or other device's behavior or an interaction with another person, such as a phone call that may be an attempt at social engineering. Employees should also understand the appropriate use for information systems and know the steps necessary should they observe another employee or contractor's behavior inconsistent

with the organization's Acceptable Use Policy. Consider that insider threats are still a common source of cybersecurity incidents, including data breaches, theft of intellectual property and sensitive information, and damage to networked systems.

Formal guidance incorporating policy and procedure is necessary to ensure people and agencies understand their roles and responsibilities as well as whom to communicate with during various phases of any event or activity. Your plans should include a stepped or phased approach to all of the considered scenarios to ensure effective and timely communication and actions between agencies.

1.2 Resources

Internal resources exterior to your immediate organization are most often very vital to the success of incident handling. Internal resource commitments should be included in your organization' Business Continuity Plan (BCP) and therefore have roles and responsibilities defined. Inner-office agencies e.g., Command & Control (C2) centers, logistics, finance and communications are required at the fundamental level to provide support for standard and contingency operations.

External resources are just as import as your internal resources. Having a comprehensive list of all partner agencies to ensure continuous communication is key to establishing and maintaining effective partnerships to foster open information sharing. Example partner agencies are:

- Federal – FBI, DHS and the National Cybersecurity & Communications Integration Center (NCCIC)
- State – MS-ISAC, Cal-CSIC and CDT
- Local – Police, Sheriff, Fire, City, Utility
- Tribal – Police, Fire, Doctrine
- Commercial – Medical, Financial, and Corporate sector associations

1.3 Personnel

When developing an Incident Response Team, it is critical to identify the various roles that make up the team: Cybersecurity personnel, IT staff, management, public relations personnel and perhaps facilities personnel if the event involves Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems. Once your IRT personnel are identified, you need to ensure they are well trained in their respective roles, which should include formal training and certification and continuing education.

2 Detection

One of the largest concerns when reporting an incident is the amount of time it takes between detecting a suspected or actual incident and notifying appropriate parties. Time sensitivity is of great concern when reporting an incident and can become critical where Personally Identifiable Information (PII) or sensitive information is involved.

An effective plan should consider and implement methods to ensure information gathered from multiple sources is effectively utilized. Information, also known as indicators, is derived from various

types of sources, both systematic and from monitored open-source information. Below are a few examples.

- **External Agency IDS/IPS.** Provides near real-time threat detection based upon rulesets developed according to an entity's cybersecurity strategy.
- **External Agency Notification.** Phone calls, email, text, postal mail and voice notification are some of the many methods of communication to consider.
- **Open Source**. Information gathered from publicly available sources as news web sites, government web sites, books, and periodicals.

Understanding how to begin to triage of an event greatly depends on the characteristics of the incident and/or events in question. There are a myriad of contributing characteristics which may demand various responses and levels of escalation.

- Authentication – unusual or unauthorized logon attempts, logon activities after hours, remote session attempts, unauthorized privilege escalation, etc.
- Data Handling – abnormal ad-hoc requests, unauthorized access or attempted access, inappropriate disclosure, inappropriate destruction of sensitive data, etc.
- Data Exfiltration – large amounts of data leaving the network by an authorized (or unauthorized) user.
- System Availability – web defacements, denial of services, hacking activities, modification of software or systems, suspicious activities
- Physical – power outages, physical damage, sabotage, physical loss or theft of information or systems
- Other – social engineering, Trojan or virus infections, harassment, elevated data disclosure, improper disposal of documents.

Next, in order to properly triage an event you must understand the impact to the operations, security classification of the information, legal implications and value of the information. Examples of some typical initial exploratory methods are:

1) Authentication: The system administrator could simply review the Security Information and Event Management (SIEM) logs to understand the account in question and reason for error and advise the ISO
2) Data Handling: The administrator can review SIEM and Active Directory logs to understand the nature of the requests – this could simply be the case of user rights management issues or it could lead to an investigation
3) Data Exfiltration: The system administrator may immediately cease all applicable activities related to the incident in question, secure their workstation or area and contact the appropriate ISO or their representative to begin preserving the information or evidence of questionable activities. Do not turn off power to the device in order to allow cybersecurity personnel to conduct forensics.
4) System Availability: The administrator may review SIEM logs to understand the activity in question and prepare to restore services from a backup and actively review firewall logs

5) Physical: Coordinate with the ISO and the facility infrastructure team to understand the nature of the event and understand how to implement secondary power and possibly provide security personnel to protect the physical perimeter and sensitive areas
6) Other: Disable the user account, take a screenshot and turn in, unplug the computer from the network, actively log authentication and access actions, etc.

There is a range of suspect security based events which could warrant an investigation based on probable cause: Authentication issues, malformed large data requests, system outages or unexplained degradation, single or multiple victims, as well as many other unexplained events. These types of events should be addressed in your IRP. In addition, your IRT should have special training in order to identify and respond appropriately to the many different types of cyber incidents such as a phishing attack, ransomware, malware, Distributed Denial of Service (DDOS).

3 Analysis

The investigation of the incident should include an Event Threat and Impact Analysis in order to categorize the impact of the event on the organization. Once the event's impact level is understood it may be appropriate to escalate the incident response and contact other entities.

The National Institute of Standards and Technology (NIST) Special Publication NIST 800-61, Computer Security Incident Handling Guide, provides advisement on prioritizing the handling of security incidents. These incidents may be applicable to computer systems as well as paper or other media. Per NIST 800-61, section 3.2.6 (Incident Prioritization) relevant factors for event threat and impact/escalation criteria include.

3.1 Impact Analysis

3.1.1 Functional Impact

Incidents may affect the confidentiality, integrity, and availability of the organization's information.

Category	Definition
None	No effect to the organization's ability to provide all services to all users.
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide some critical services to any users.

Table 2 - Examples of Functional Impact Categories

3.1.2 Information Impact

Incidents may affect the confidentiality, integrity, and availability of the organization's information.

Category	Definition
None	No information was exfiltrated/leaked, disclosed, changed, deleted, used, or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc., was accessed or exfiltrated/leaked, or protected health information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes.
Integrity Loss	Sensitive or proprietary information was changed or deleted accidentally or intentionally.

Table 3 - Possible Information Impact Categories

3.1.3 Recoverability

The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly); launch investigation.

Table 4 - Recoverability Effort Categories

3.2 Types of Threat

Your analysis of the incident should include considerations relative to the specific type of threat. Each type of attack may require a different response. For example a ransomware attack involves a much different response than a Distributed Denial of Service attack.

3.3 Physical Considerations

Any incident involving or affecting physical systems or critical infrastructure mandates the participation of the applicable Critical Infrastructure Protection (CIP) team(s). Incidents involving physical infrastructures have additional considerations in addition to the typical cyber related attacks. Now CIP centric organizations have to consider more than simply network protection principles; they must also take into consideration the acquisition and replacement of systems on the network.

The Federal Energy Regulatory Commission (FERC) Order 829 mandated additional controls addressing cyber security supply chain risk management for ICS hardware, software and computing services associated with Bulk Electric Systems (BES).

3.3.1 North American Electric Reliability Corporation (NERC) Standards

The North American Electric Reliability Corporation (NERC) created implementation guidance CIP-013-01 to assist with Supply Chain Risk Management. There are many other NERC sponsored standards that may also apply and warrant heavy consideration.

CIP-002-5.1a	Cyber Security — BES Cyber System Categorization		Subject to Enforcement
CIP-003-6	Cyber Security - Security Management Controls	Related Information	Subject to Enforcement
CIP-004-6	Cyber Security - Personnel & Training	Related Information	Subject to Enforcement
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	Related Information	Subject to Enforcement
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Related Information	Subject to Enforcement
CIP-007-6	Cyber Security - System Security Management	Related Information	Subject to Enforcement
CIP-008-5	Cyber Security - Incident Reporting and Response Planning	Related Information	Subject to Enforcement
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	Related Information	Subject to Enforcement
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments	Related Information	Subject to Enforcement
CIP-011-2	Cyber Security - Information Protection	Related Information	Subject to Enforcement
CIP-014-2	Physical Security	Related Information	Subject to Enforcement

Table 5 – Sample NERC Standards

3.3.2 Other Physical Considerations

3.3.2.1 Physical considerations extend beyond the immediate physical and boundary of the computing center; even beyond the facility walls. Physical considerations encompass any and all physical and / or mechanical features directly or indirectly required to support business operations. Some example areas of concern that may require addition consideration:

3.3.2.2 Environmental Control Systems (ECS) are required to maintain an environment conducive to static free temperature and humidity controlled environment. These controllers are more often than not enabled with an Internet or network connection which inherently creates additional vulnerabilities and risk to the environment.

3.3.2.3 Bulk Electrical Systems (BES) require additional considerations during the Post-Incident or Recovery phase of an incident in addition to the "typical" cyber related business recovery actions. BES systems inherently have additional physical recovery considerations to ensure the proper restoration to protect the confidentiality, integrity and the availability of public and private critical physical infrastructure.

3.3.2.4 The Federal Energy Regulatory Commission (FERC) Order 829 mandated additional controls addressing cyber security post-incident recovery for ICS hardware, software and computing services associated with Bulk Electric Systems (BES). The North American Electric Reliability Corporation (NERC) created implementation guidance CIP-009-6 , as part of the overall CIP-009 recovery plan, to provide guidance with national, state and local CIP recovery strategies. More information is available directly from the NERC website at http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

3.3.2.5 Security of the facility and applicable supporting infrastructure is another vital area concern. Recovery efforts must include ensuring the physical and / or logical boundaries are "sound" and free of "evidence of tamper". The organization may no longer have the resources necessary to secure the environment, and therefore may look into other options such as contracted support. This type of action may require support by contracting, financial, logistics and management personnel.

4 Containment

Organizations are responsible to develop and employ sufficient methodologies to contain the incident in order to minimize continued impact and / or disruption of services to the organization as well as reducing the possibility of continued contamination to other services. Tactics supporting the immediate local isolation and containment are vital to slowing, and hopefully stopping the proliferation of the attack. However this approach is only one part of a multi-faceted approach.

The containment plans are usually based on the findings of the security team's investigation of the incident. Often times, the plan relies on limited information gathered during the preliminary detection.

ISO and recovery teams must ensure they don't fall into this stove piped, single source technique of information analysis. Information is acquired from multiple sources based on the attack vector.

A risk management strategy should address the risk at every level, starting with the infected computing device all the way to examining the viability of the network. During the investigative phase and beyond, the affected computing devices may require immediate isolation or removal from the network in order to support the required efforts. Some commonly employed network tactics involve disconnecting or isolating network segments, creating additional firewall rules, employing active IDS / IPS rules or simply disconnecting the infected network from the company and / or public networks.

5 Eradication

Beyond the identification and containment, there is the requirement to determine how to effectively and safely remove the source of the incident from the computing device and ensure another node in your network is not affected in the future. Many companies stop at removing the device from the network and stop there; remember malware spreads silently and very rapidly. The eradication process must include measures to not only remove the infection from the primary device, but various methods to scan every device on the affected network segment to ensure the relevant risk is addressed.

6 Recovery

Today's technological and business environments are dynamic and utilize multiple platforms for information management. A company must ensure they understand their technological boundaries and considers recovery principles and methodologies for every environment. Information Technology Recovery Plans are essential and should align with the Incident Response Plan.

6.1 Data Recovery

The key to an effective data recovery strategy begins with a well planned and executed backup strategy. A back-up strategy may vary from company to company based on the data type, location, sensitivity, availability requirements, and / or data owners. Other variables may come into play such as location of the backup media or the SOW with an external data recovery vendor. Prior to any data restoration activities, the data owners should confirm with the data custodians of all the previous and current locations of any live or backup data.

6.2 Service Recovery

Recovery expectations and deliverables are typically spelled out within the Service Level Agreement (SLA) in a service contract. There are two main service categories organizations should have situational knowledge of, Platform as a Service (PAAS) or Infrastructure as a Service (IAAS).

6.3 Site Recovery

Site recovery is typically defined within your Business Continuity Plan (BCP) and may be needed in the Data Recovery Plan (DRP) or Technology Recovery Plan (TRP). The actions required for site recovery are based upon what type of recovery site is defined in the BCP, e.g., cold site, warm site or hot site.

7 Post-Incident Activity

The Computer Security Incident Handling Guide (NIST 800-61) provides advisement on event analysis activities. Relevant factors for post-incident and root cause analysis include:

7.1 Lessons Learned

1) **Learning and improving.** Incident Response Teams should hold "lessons learned" meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:
   a) Exactly what happened, at what times?
   b) How well did staff and management perform? Were documented procedures followed? Were procedures adequate?
   c) What information was needed sooner?
   d) Were any steps or actions taken that might have inhibited the recovery?
   e) What would staff and management do differently the next time a similar incident occurs?
   f) How could information sharing with other organizations have been improved?
   g) What corrective actions can prevent similar incidents in the future?
   h) What precursors or indicators should be watched for in the future to detect similar incidents?
   i) What additional tools or resources are need to detect, analyze, and mitigate future incidents?

2) **Follow-up reporting.** An important post-incident activity is creating a follow-up report for each incident. Report considerations include:
   a) Creating a formal event chronology (including time-stamped information from systems);
   b) Compiling a monetary estimate of the amount of damage the incident caused;
   c) Retaining follow-up reports as specified in retention policies.

3) **Data collected.** Organizations collect data that is actionable and decide what incident data to collect based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event. Accountable authorities should make a determination on data retention and disposition.

4) **Root Cause Analysis.** Organizations performing root cause analysis should focus on relevant objective assessment activities including:
   a) Reviewing of logs, forms, reports, and other incident documentation;
   b) Identifying recorded precursors and indicators;
   c) Determining if the incident caused damage before it was detected;
   d) Determining if the actual cause of the incident was identified;
   e) Determining if the incident is a recurrence of a previous incident;
   f) Calculating the estimated monetary damage from the incident;
   g) Measuring the difference between initial impact assessment and the final impact assessment;
   h) Identifying measures, if any, that could have prevented the incident.

7.2 Recommendations

The entity should compose a report based on the lesson(s) learned and any shortfalls identified during the incident handling and reporting process. This information is then used to:

(1) Update the Incident Response Plan
(2) Retrain the Incident Response Team as necessary
(3) Provide a written record of the incident
(4) Share with cybersecurity partners for them to use as lessons learned

8 Other Response Activities

Threat response activities may require encompass many resources and capabilities law enforcement. Threat response activities during a cyber-incident include investigative, forensic, analytical, and mitigation activities; interdiction of a threat actor; and providing attribution that may lead to information sharing and operational synchronization with asset response activities. Threat response activities also include conducting appropriate law enforcement and national security investigative activities at the affected entity's site, linking related incidents, and identifying additional affected or potentially affected entities. The SLTTP community plays important roles in working with respective law enforcement entities on threat response. State and Federal agencies with intelligence functions, such as those of Cal-OES, DHS, DOJ, DoD, Department of Energy (DOE), and members of the State and Federal Intelligence Communities (IC), may perform a substantial threat response role when a significant cyber incident affects their duties or responsibilities, or there is suspicion of activities conducted by a foreign power or agent of a foreign power.

8.1 Incident Reporting

The following reporting actions for the ISO should happen in the order depicted; however they could happen simultaneously based on the questionable activity / incident:

1) Report the incident within your organization in accordance with approved incident response plan reporting procedures. Ensure you adhere to all entity prescribed practices prior to, or in conjunction with the following procedures.
2) Contact the appropriate law enforcement agency e.g., city, county, state, or federal as applicable. Begin with contacting your local law enforcement agency for assistance if the activity appears criminal in nature.
3) Contact the appropriate State level cybersecurity organization. Refer to the California Joint Cyber Incident and Escalation Framework for detailed contact information.

8.2 Notification

Establish and maintain a unified and coordinated operational structure and process that appropriately integrates critical stakeholders and supports execution of core capabilities. This is the capability to conduct actions and activities that enable decision makers to determine appropriate courses of action and to provide oversight for complex operations. Operational coordination, in accordance with the

principles of the National Incident Management System (NIMS) and the Incident Command System (ICS), coordinates the threat response, asset response, and intelligence support activities in the face of a cyber threat. All entities should incorporate ICS and NIMS principles into their IRP.

In the context of a cyber incident, incident notification includes efforts to coordinate activities across and among all levels of government and with private sector partners. This involves national operations centers, as well as on-scene response activities that manage and contribute to multi-agency efforts.

Certain types of breaches carry legal notification responsibilities. This section includes information about breach notification statutes and rules according to California law, federal laws and regulations, and other states' laws as depicted by the National Conference of State Legislatures.

Code	Title	Definition	Link
California Civil Code 1798.29, Article 7,	Accounting of Disclosures	Any government agency that maintains computerized data that includes personal information that the agency does not own should notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	California Civil Code Link
California Civil Code 1798.80, Title 1.81	Customer Records	"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	California Civil Code Link

Table 6 - California Civil Code for Notifications

Various Federal agencies may impose additional reporting requirements based upon the information type, categorization and / or classification of the information. Reporting timelines and formats more often than not also vary based upon specific agency reporting requirements. Ensure your reporting methodologies take all agency considerations into play when developing reporting procedures.

Breach Notice	Citation	Requirement	Notes
HIPAA	45 CFR §164.404	Notify individual or Covered Entity of a breach of unsecured protected health information which poses a significant risk of financial, reputational, or other harm to the individual. Individual notice must contain certain mandatory media notices (involving 500 or more individuals) as soon as possible but no later than 60 days from discovery of the breach.	Applies only to HIPAA Covered Entities and HIPAA-protected health information. A Business Associate of a Covered Entity is required to notify the Covered Entity as soon as possible but no later than 60 days from the discovery of the breach. Contracting for a shorter time is a best practice.
Federal Financial Participation	CMS SMDL #06-022	CMS-regulated entities must notify CMS within one clock hour according to Sep. 2006 CMS letter to State Medicaid Directors	SNAP, TANF, and CHIP each have similar authorizations to use or disclose Medicaid information that identifies an applicant or recipient is limited to use or disclosure "directly in connection with program administration," but no breach notice requirement.
Internal Revenue Service	By data sharing agreement with the IRS, pursuant to IRS Publication 1075 §10	Notify IRS Office of Safeguards of compromised IRS or SSA data within one clock hour from discovery of an actual or suspected breach. Follow individual agency procedures for notifying impacted individuals.	The IRS Office of Safeguards may require individual notification.
Social Security Administration (SSA)	By contract between SSA and Agency which defers to IRS Publication 1075	Notice required to SSA within one clock hour of discovery. Follow instructions of SSA to notify impacted individuals, if any.	SSA may require individual notification.
Federal Trade Commission (FTC)	Health Breach Notification (PHR, EHR Vendors) 16 CFR	Requires a vendor of personal health records to notify the individual US Citizen and the FTC following	Applies to foreign and domestic vendors of personal health records, PHR-related entities, and third-party

	Part 318	the discovery of a breach of security of unsecured PHR-identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR-related entity.	service providers, irrespective of any jurisdictional tests in the FTC Act, that maintain information of US citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. "Breach" is acquisition unauthorized by the individual. Notify without unreasonable delay and in no case later than 60 calendar days after the breach discovery.
Family Educational Rights and Privacy Act (1974)	20 USC §1232g, 34 CFR Part 99	None. FERPA guidance recommends having breach response plans.	Applies to educational institutions regarding the privacy of personally identifiable information contained in education records of students. Consent generally is required to disclose education records.

Table 7 - Additional Agency Reporting Requirements

8.3 Escalation

NIST 800-61 Computer Security Incident Handling Guide provides advisement on escalation of security incidents. Section NIST 800-61, 3.2.7 (Incident Notification) outlines important contacts and modes of communications.

8.3.1 CCIU and Cal-CSIC Response

The CCIU and Cal-CSIC may automatically engage in escalation procedures based upon the criticality level described in accordance with the *California Joint Incident Communications Framework.*

- Level 3 Actions (ESF-18)
  This criticality category of incidents typically will inconvenience the agency with the potential to cause some type of degradation to service if left unattended or improperly handled. Incidents at this criticality would demand coordination between the reporting agency and:
  - State CISO
  - Reporting Agency AISO / ISO or Executive Leadership
  - Reporting Agency AIO / CIO or Executive Leadership

- Level 2 Actions (ESF-18)

Incidents associated with this criticality typically cause a recoverable service or process degradation OR have the potential to have a monumental impact on the agency. Incidents at this criticality would demand coordination between the reporting agency and:

- State CISO
- Reporting Agency AISO / ISO or Executive Leadership
- Reporting Agency AIO / CIO or Executive Leadership
- Federal Partners

- Level 1 Actions (ESF-18)
  Any cyber related incident designated with a DHS Severity rating of "Level 5 Emergency" or a California Cyber Incident Severity rating of "Level 3 (Black)" requires additional immediate considerations. An incident of this severity indicates an actual or potential impact on public health, welfare or the states network infrastructure. Incidents at this criticality would demand coordination between the reporting agency and:
  - State CISO
  - Reporting Agency AISO / ISO or Executive Leadership
  - Reporting Agency AIO / CIO or Executive Leadership
  - California Government Operations Secretary
  - Reporting Agency Secretary or SLTTP Executive Leadership
  - Federal Partners
  - Public / Private Partnerships
  - Governor's Office

8.3.2 Key Contacts

Organizations should establish an escalation process for instances when key individuals outside of normal technical response processes must be notified. Among those to be considered are:

- CIO or Information Resources Manager
- CISO or Information Security Officer
- CPO or Privacy Officer
- Other incident response teams within the organization
- External (contractor) incident response teams, if appropriate
- System owner
- Human resources
- Public affairs
- Legal department
- US-CERT (required for systems operated on behalf of the federal government)
- Law enforcement, if appropriate
- Federal government agencies, if appropriate

8.3.3 Methods of Contact

Organizations may need to provide status updates to certain external and internal parties. Among communication methods to be considered are:

- Telephone calls
- Website (internal, external, or portal)
- Email
- In person (e.g., daily briefings)
- Voice mailbox greetings (e.g., set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status; use the help desk's voice mail greeting)
- Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points)

Appendices

Appendix A – Glossary

Admissible Evidence: evidence that is accepted as legitimate in a court of law, *see* Chain of Custody.

Authentication: security measure designed to establish the validity of a transmission, message, or originator, or the identity confirmation process used to determine an individual's authorization to access data or computer resources.

Authorized User: a person granted certain permissions to access, manage, or make decisions regarding an information system or the data stored within.

Authorized Use and Disclosure: a permissible action or use of **Confidential Information**.

Authorization: the act of granting a person or other entity permission to use data or computer resources in a secured environment.

Availability: assurance that the systems responsible for delivering, storing, and processing information are accessible when needed by those who need them.

Breach: an impermissible use or disclosure by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of **Confidential Information** such that the use or disclosure poses a significant risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Depending upon applicable law, "Breach" may for example mean:

1) HIPAA Breach of Protected Health Information ("PHI"). With respect to PHI pursuant to HIPAA Privacy and Breach Notification Regulations and regulatory guidance any unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Regulations is presumed to be a Breach unless a Covered Entity or Business AISOciate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Compromise will be determined by a documented Risk Assessment including at least the following factors:
    a. The nature and extent of the **Confidential Information** involved, including the types of identifiers and the likelihood of re-identification of PHI;
    b. The unauthorized person who used or to whom PHI was disclosed;
    c. Whether the Confidential Information was actually acquired or viewed; and
    d. The extent to which the risk to PHI has been mitigated.

    With respect to PHI, a "Breach" pursuant to HIPAA Breach Regulations and regulatory guidance *excludes*:
    a. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business AISOciate if such acquisition, access, or use was made in good faith and within the scope of authority, and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations.
    b. Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business AISOciate location to another person authorized to access PHI at the same Covered Entity or Business AISOciate, or organized health care arrangement as defined by HIPAA in which the Covered Entity participates, and the information received as a result of

such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations

c. A disclosure of PHI where a Covered Entity or Business AISOciate demonstrates a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, pursuant to HIPAA Breach Regulations and regulatory guidance.

2) Breach in California. Breach means "Breach of System Security," applicable to electronic Sensitive Personal Information (SPI) that compromises the security, confidentiality, or integrity of Sensitive Personal Information. Breached SPI that is also PHI may also be a HIPAA breach, to the extent applicable.
3) Any unauthorized disclosure as defined by any other law and any regulations adopted thereunder regarding **Confidential Information**.

Business Continuity Plan: the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

Chain of Custody: refers to the application of the legal rules of evidence and its handling.

Confidential Information: any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) that consists of or includes any or all of the following:

1) Federal Tax Information, sourced from the Internal Revenue Service (IRS) under an IRS data sharing agreement with the agency;
2) Personally Identifiable Information;
3) Sensitive Personal Information;
4) Protected Health Information, whether electronic, paper, secure, or unsecure;
5) Social Security Administration data, sourced from the Social Security Administration under a data sharing agreement with the agency;
6) All non-public budget, expense, payment, and other financial information;
7) All privileged work product;
8) Information made confidential by administrative or judicial proceedings;
9) All information designated as confidential under the laws of the State of California and of the United States, or by agreement; and
10) Information identified in a contract or data use agreement to which an agency contractor specifically seeks to obtain access for an Authorized Purpose that has not been made public.

Confidentiality: assurance that information is not disclosed to system users, processes, and devices unless they have been authorized to access the information.

Containment: the process of preventing the expansion of any harmful consequences arising from an Incident.

Contingency Management Plan: a set of formally approved, detailed plans and procedures specifying the actions to be taken if or when particular circumstances arise. Such plans should include all eventualities ranging from key staff absence, data corruption, loss of communications, virus infection, partial loss of system availability, etc.

Data: information in an oral, written, or electronic format that allows it to be retrieved or transmitted.

Disaster Recovery Plan: a crisis management master plan activated to recover IT systems in the event of a disruption or disaster. Once the situation is under control, a Business Continuity Plan should be activated.

Discovery: the first time at which an event is known, or by exercising reasonable diligence should have been known, by an officer, director, employee, agent, or agency contractor, including events reported by a third party to an agency or agency contractor.

Encryption: the process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes. A "key" (e.g., a password of some sort) is necessary to decrypt the data and return it to its original state. Applicable law may provide for a minimum standard for compliant encryption, such as HIPAA or NIST standards.

Eradication: the removal of a threat or damage to an information security system.

Event: an observable occurrence in a network or system or of confidential information.

Forensics: the practice of gathering, retaining, and analyzing information for investigative purposes in a manner that maintains the integrity of the information.

Hacker: unauthorized user who attempts to or gains access to an information system.

Hardware: the physical technology used to process, manage, store, transmit, receive, or deliver information. The term does not include software. Examples include laptops, desktops, tablets, smartphones, thumb drives, mobile storage devices, CD-ROMs, and access control devices.

Harm: although relative, the extent to which a privacy or security incident may actually cause damage to an agency or harm to an individual, reputation, financial harm, or results in medical identity theft.

Incident: an attempted or successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system.

Incident Response Lead: person responsible for the overall information security Incident management within an agency and is responsible for coordinating the agency's resources which are utilized in the prevention of, preparation for, response to, or recovery from any Incident or Event.

Incident Response Team (IRT): led by the Incident Response Lead, the core team composed of subject-matter experts and information privacy and security staff that aids in protecting the privacy and security of information that is confidential by law and provides a central resource for an immediate, effective, and orderly response to Incidents at all levels of escalation.

Information Security: the *administrative, physical,* and *technical* protection and safeguarding of data (and the individual elements that comprise the data).

Integrity: assurance that the data are authentic, accurate, and complete and can be relied upon to be sufficiently accurate for their purpose.

Local Area Network (LAN): a private communications network owned and operated by a single organization within one location.

Malicious Code: a software program that appears to perform a useful or desirable function but actually gains unauthorized access to computer system resources or deceives a user into executing other malicious logic.

Malware: a generic term for a number of different types of malicious code.

Penetration: gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Protected Health Information (PHI): information subject to HIPAA: Individually identifiable health information in any form that is created or received by a HIPAA Covered Entity, and relates to the individual's healthcare condition, provision of healthcare, or payment for the provision of healthcare as further described and defined in the HIPAA Privacy Regulations. PHI includes:

- demographic information unless such information is De-identified as defined in the HIPAA Privacy Regulations;
- "Electronic Protected Health Information" and unsecure PHI as defined in the HIPAA Privacy Regulations;
- the PHI of a deceased individual within 50 years of the date of death; and
- employment information.

Personal Identifying Information (PII): Under California Civil Code4 §1798.80 81
"Personal information" means any information that identifies, relates to, describes or is capable of being associated with a particular individual, including, but not limited to:

- name, address, social security number, date of birth;
- government-issued identification number; driver's license; state ID card;
- mother's maiden name; signature, medical information; insurance information;
- unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
- unique electronic identification number, address, or routing code; banking information;
- credit card / debit card information, education, employment (current and/or history).

Privacy: the right of individuals to keep information about themselves to themselves and away from others. For example, privacy in the healthcare context means the freedom and ability to share an individual's personal and health information in private.

Protocol: a set of formal rules describing how to transmit data, especially across a network.

Recovery: process of recreating files which have disappeared or become corrupted from backup copies.

Reportable Event: an event that involves a breach of Confidential Information requiring legal notification to individuals, government authorities, the media, or others.

Risk Assessment: the process by which the potential for harm is identified and the impact of the harm is determined.

Sensitive Data: while not necessarily protected by law from use or disclosure, data that is deemed to require some level of protection as determined by an individual agency's standards and risk management decisions. Some examples of "Sensitive Data" include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Internal communications
- Information determined to be authorized for use or disclosure only on a "need-to-know" basis

Server: A multi-processing computer that supplies a network of less powerful machines (such as desktop PCs and laptop computers) with applications, data, messaging, communication, information, etc.

Sensitive Personal Information (SPI):

1) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and items are not encrypted:
    a. Social security number;
    b. Driver's license number or government-issued identification number; or
    c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
2) Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual;
    b. The provision of health care to the individual; or
    c. Payment for the provision of health care to the individual.

Threat: any circumstance or event with the potential to adversely impact an information system through the unauthorized access, destruction, disclosure, modification of data and/or denial of service.

Vulnerability: weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

Wide Area Network (WAN): a communications network that extends beyond the organization's immediate premises.

Appendix B – Acronyms

CDO: Chief Data Officer

CFAA: Computer Fraud and Abuse Act (1986)

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CJIS: Criminal Justice Information Services, a division of the FBI

CPO: Chief Privacy Officer

CTO: Chief Technology Officer

FISMA: Federal Information Security Management Act (2002)

FOIA: Freedom of Information Act

FTI: Federal taxpayer information

HIPAA: Health Insurance Portability and Accountability Act (1996)

IRS: Internal Revenue Service

IRT: Incident Response Team

ISO: Information Security Office

IT: Information Technology

NIST: National Institute of Standards and Technology

PHI: Personal Health Information

PIA: Public Information Act,

PII: Personally Identifiable Information

PRA: Public Records Act, California Government Code §§ 6250 through 6276.48

RFI: Request for Information

SOC: Security Operations Center

SPI: Sensitive Personal Information

SSA: Social Security Administration

TTP: Tactics, Techniques and Protocols

Appendix C – Federal Laws and Regulations for Data Privacy and Security

Guidance	Description	Location
Health Insurance Portability and Accountability Act (HIPAA) (1996)	**HIPAA contains the following provisions regulating the use and disclosure of protected health information:** • ***Privacy Rule* protects the privacy of individually identifiable health information;** • ***Security Rule* sets national standards for the security of electronic protected health information;** • ***Breach Notification Rule* requires covered entities and business AISOs to provide notification following a breach of unsecured protected health information;** • ***Enforcement* providing civil and criminal penalties for violation; and** • ***Patient Safety Rule* protects identifiable information being used to analyze patient safety events and improve patient safety.**	**HIPAA (1996);**
Health Information Technology for Economic and Clinical Health Act (HITECH) (2009)	HITECH amended HIPAA in 2009 with interim regulations, expanding direct liability to HIPAA Business AISOs and requiring Covered Entities and Business AISOs to report data breaches to those affected individuals through specific breach notification requirements.	HITECH (2009) (ARRA Title XIII)
HIPAA Omnibus Regulations (2013)	These regulations made substantial changes to HIPAA: • The Omnibus Regulations finalized the interim HITECH regulations; • Made Business AISOs directly liable for certain Privacy and Security requirements; • Enacted stronger prohibitions on marketing (opt-out) and sale of Protected Health Information (PHI) without authorization; • Expanded individuals' rights to receive electronic copies of PHI; • Allowed individuals the right to restrict disclosures to a health plan concerning treatment for which the individual has paid out-of-pocket in full; • Required Notice of Privacy Practices updates and redistribution; • Changed authorization related to research and disclosure of school proof of child immunization and access to decedent information by family members or others; • Enhanced enforcement in many ways, including addressing the enforcement against noncompliance with HIPAA Rules due to willful neglect; • Finalized the rule adopting changes to the HIPAA Enforcement Rule to incorporate tiered, mandatory penalties up to $1.5 million per violation; and • Finalized rule adopting GINA and prohibited most health plans from using or disclosing genetic information for underwriting purposes, as proposed in Oct. 2009.	45 CFR Parts 160-164
Family Educational Rights and Privacy Act (FERPA) (1974)	FERPA creates a right of privacy regarding grades, enrollment, and billing information. Specifically, this information may not be released without prior consent from the student. In addition to safeguarding individual student records, the law also governs how state agencies transmit testing data to federal agencies.	20 USC § 1232G; 34 CFR Part 99

Federal Information Security Management Act (FISMA) (2006)	Federal legislation that assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to provide for the strengthening of information security systems. Specifically, the Act requires heads of each agency to implement policies and procedures to effectively and efficiently drive down IT security issues to acceptable levels through a defined framework by which federal government agencies would ensure the security of information systems controlled by either the agency or one of its contractors on behalf of a federal agency. The framework is further defined by the standards and guidelines set forth by NIST.	44 USC §§ 3541-3549
Internal Revenue Service Statute and Regulation	Through Publication 1075, the IRS has created a framework by which Federal Tax Information (FTI) and Personally Identifiable Information (PII) is protected from public disclosure. To ensure the safety of such data, receiving agencies and/or entities must have proper safeguards in place. Federal code requires external agencies and other authorize recipients of federal tax return and return information (FTI) to establish specific procedures to ensure the adequate protection of the FTI they receive. In addition, the same section of the Code authorizes the IRS to suspend or terminate FTI disclosure to a receiving agency or other authorized recipient if misuse or insufficient FTI safeguards are found. In addition to criminal sanctions, the Internal Revenue Code prescribes civil damages for unauthorized disclosure and, when appropriate, the notification to affected taxpayers that an unauthorized inspection or disclosure has occurred.	Publication 1075; IRC Section 6103(p)(4); 26 USC §6103(p)(4)
Social Security Administration (SSA) Statute and Regulation	Much of the information SSA collects and maintains on individuals is especially sensitive, therefore prior to disclosing of such information, SSA must look to the Privacy Act of 1974, 5 USC Section 552a, FOIA, 5 USC Section 1106 of SSA, 42 USC Section 1306. SSA employees are prohibited from disclosing any information contained in SSA records unless disclosure is authorized by regulation or otherwise required by federal law. SSA may only disclose personal records (PII) when the individual to whom the record pertains provides written consent or when such disclosure falls into one of the several narrowly-drawn exceptions.	Privacy Act of 1974; 5 USC Section 552a; FOIA; 5 USC §1106 (SSA); 42 USC §1306
National Institute of Standards and Technology (NIST)	NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and to help with managing cost effective programs to protect their information systems and the data stored on the systems. NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in FIPS 200. The security rule covers 17 areas, including control, incident response, business continuity, and disaster recoverability. A key part of the certification and accreditation process for federal information systems is selecting and implementing a subset of the controls. Agencies are expected to comply with NIST security standards and guidelines.	NIST 800-53 rev. 4; FIPS 200
Criminal Justice	CJIS is a division of the FBI that compiles data provided by law	CJIS Security

Information Services (CJIS)	enforcement agencies across the United States. CJIS is the world's largest repository of criminal fingerprints and history records which can be accessed and searched by law enforcement to enable the quick apprehension of criminals. The responsibility of CJIS extends to the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Incident-Based Reporting System (NIBRS). In addition to its many responsibilities in the coordination and sharing of criminal data, CJIS promulgates the CJIS Security Policy, which is meant to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI). The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. The policy applies to every individual – contractor, private entity, noncriminal justice agency representatives, or members of a criminal justice entity – with access to, or who operate in support of, criminal justice services and information.	Policy, TGC § 552.108
Clinical Laboratory Improvements Amendments (CLIA)	CLIA are federal regulatory standards applying to clinical laboratory testing performed on humans in the United States. The CLIA Program sets standards and issues certificates for clinical laboratories. The objective of CLIA is to ensure the accuracy, reliability, and timeliness of test results regardless of where the test is performed. All clinical laboratories must be properly certified to receive Medicare and Medicaid payments. The primary responsibility for the administration of this program is held by the Centers for Medicare and Medicaid Services.	CLIA Regulations and Guidance
Computer Fraud and Abuse Act (CFAA)	CFAA is a federal law passed to address computer-related crimes. The Act governs cases with a compelling federal interest; where computers of the federal government or certain financial institutions are involved; where the crime is interstate in nature; or where computers are used in interstate and foreign commerce. The CFAA defines "protected computers" as those exclusively used by financial institutions or the US Government, or when the conduct constituting the offense affects the use by or for the financial institution or the federal government, or those computers which are used in or affecting interstate or foreign commerce or communication.	18 USC §1030

Appendix D – Federal Contacts

Resource	Services	Contact Information
Federal Bureau of Investigation	Cyber squads in each field office investigate high-tech crimes, including computer intrusions and theft of personal information.	California Field Offices **Sacramento**: 2001 Freedom Way Roseville, CA 95678 Phone: (916) 746-7000 **San Francisco:** 450 Golden Gate Avenue, 13th Floor San Francisco, CA 94102-9523 sanfrancisco.fbi.gov Phone: (415) 553-7400 **Los Angeles**: 11000 Wilshire Boulevard Suite 1700 Los Angeles, CA 90024 losangeles.fbi.gov Phone: (310) 477-6565 **San Diego**: 10385 Vista Sorrento Parkway San Diego, CA 92121 sandiego.fbi.gov Phone: (858) 320-1800
Federal Emergency Management Agency (FEMA)	Provides disaster response and recovery assistance.	1-800-621-FEMA (3362)
National Cyber Security Division (NCSD), US Dept. of Homeland Security	Works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.	Response coordination: (202) 282-8000
CERT Coordination Center (CERT/CC)	Federally-funded CERT provide technical advice to federal, state, and local agencies on responses to security compromises.	CERT 24-hour hotline: (412) 268-7090 forensics@cert.org
US Secret Service	Investigates financial crimes, including identity theft.	**Sacramento Field Office:** 501 I Street, #12100 Sacramento, CA, 95814-2322 **Phone:** (916) 325-5481 **San Jose Field Office:** 28 0 S First Street, #1111 San Jose, CA, 95113 **Phone:** (408) 535-5288 **Fresno Field Office:** 52 00 North Palm Avenue, #207 Fresno, CA, 93704 **Phone:** (559) 487-5204
US Treasury Inspector General for Tax	Works with agencies to ensure that all appropriate actions are taken with regard to Federal Tax Information.	TIGTA Field Division, Dallas: (972) 308-1400

Administration (TIGTA) and Office of Safeguards		
Federal Trade Commission (FTC)	Regulates consumer business practices.	http://www.ftc.gov Detecting identity theft: http://www.ftc.gov/idtheft
National Institute of Standards and Technology (NIST), US Dept. of Commerce	Advances US measurement science, standards, and technology, including accelerating the development of and deployment of standards and systems that are reliable, usable, interoperable, and secure. Assigned certain information security responsibility under the Federal Information Security Management Act of 2002 (FISMA, 44 USC § 3541, *et seq.*). NIST has published over 200 information security documents on information security standards, guidelines, and other resources necessary to support the federal government.	Main office: (301) 975-NIST inquiries@NIST.gov http://www.nist.gov/index.html Publications: http://csrc.nist.gov/publications/
Office for Civil Rights (OCR), US Dept. of Health and Human Services	Oversees federal civil rights and health information privacy, security, and breach notice by HIPAA.	http://www.hhs.gov/ocr/office/index.html
US Postal Service Inspector Service	The law enforcement arm of the US Postal Service, which investigates crimes that may adversely affect or fraudulently use the US Mail, the postal system, or postal employees.	https://postalinspectors.uspis.gov